Q) <u>HomeWork:-</u> Show that for all primes p Q(P) is an integer where

$$Q(P) = \prod_{K=1}^{P-1} \left(K^{2K-P-1} \right)$$

Ans:- $\binom{P}{K}$ is an integer for all $K \leq P$

$$Q(p) = \frac{\left(1^1 \cdot 2^2 \cdot 3^3 \cdots (p-1)^{p-1}\right)^2}{\left(1 \cdot 2 \cdots (p-1)\right)^{p+1}}$$

$$Q(p) = 1^{2\times 1 - p - 1} \; 2^{2\times 2 - p - 1} \; 3^{2\times 3 - p - 1} \; (p-1)^{2\times(p-1) - p - 1}$$

$$= \frac{(1)^2}{1^{p+1}} \frac{(2^2)^2}{2^{p+1}} \frac{(3^3)^2}{3^{p+1}} \cdots \frac{\left((p-1)^{p-1}\right)^2}{(p-1)^{p+1}}$$

$$= \frac{\left(1^1 \cdot 2^2 \cdot 3^3 \cdots (p-1)^{p-1}\right)^2}{\left(1 \cdot 2 \cdot 3 \cdots (p-1)\right)^{p+1}} = \frac{N}{D}$$

$$D = \left((p-1)!\right)^{p+1}$$

$$N = \left(1 \cdot 2 \cdot 2 \; 3 \; 3 \cdot 3 \; \cdot \; \underbrace{(p-1) \cdots (p-1)}_{(p-1) \text{ times}}\right)^2$$

$$\Rightarrow N = \Big((1 \cdot 2 \cdot 3 \; \cdot p-1)(2 \; 3 \cdots (p-1))(3 \cdot 4 \; \cdot (p-1))(4 \cdot 5 \cdots (p-1))$$

$$\cdots ((p-2)(p-1))((p-1)) \Big)^2$$

$$\Rightarrow N = \left((p-1)! \; \frac{(p-1)!}{1!} \; \frac{(p-1)!}{2!} \; \frac{(p-1)!}{3!} \cdots \frac{(p-1)!}{(p-2)!} \right)$$

$$\Rightarrow N = \left(\frac{\left((p-1)!\right)^{p-1}}{1! \; 2! \; 3! \cdots (p-2)!} \right)^2$$

$$Q(p) = \frac{N}{D} = \left(\frac{\left((p-1)!\right)^{p-1}}{1! \; 2! \; (p-2)!} \right)^2 \times \frac{1}{\left((p-1)!\right)^{p+1}}$$

$$= \left((p-1)!\right)^{2p-2-p-1} \left(\frac{1}{1! \; 2! \cdots (p-2)!} \right)^2$$

$$\;^{p-3} \left(\frac{1}{\quad} \right)^2$$

$$= ((p-1)!) \quad (1! \, 2! \cdots (p-2)!)$$

$$= ((p-1)!)^{p-3} \left(\frac{1}{1! \, 2! \cdots (p-2)!} \right)^2$$

$$= ((p-1)!)^{p-1} \left(\frac{1}{1! \, 2! \cdots (p-1)!} \right)^2$$

$$= \frac{1}{p^{p-1}} (p^{p-1}) ((p-1)!)^{p-1} \left(\frac{1}{1! \, 2! \cdots (p-1)!} \right)^2$$

$$= \frac{1}{p^{p-1}} (p!)^{p-1} \left(\frac{1}{1! \, 2! \cdots (p-1)!} \right)^2$$

$$= \left(\frac{1}{p} \frac{p!}{1!(p-1)!} \right) \left(\frac{1}{p} \frac{p!}{2!(p-2)!} \right) \cdots \left(\frac{1}{p} \frac{p!}{(p-1)!1!} \right)$$

$$= \prod_{k=1}^{p} \left(\frac{\binom{p}{k}}{p} \right)$$

Now $\dfrac{\binom{p}{k}}{p} \in \mathbb{Z}$ as in Number Theory 5 notes

$\Rightarrow Q(p) \in \mathbb{Z}$

Q) $F_n = 2^{2^n} + 1$ and $F_m = 2^{2^m} + 1$ Show that F_n & F_m are coprime $\forall\, m, n \in \mathbb{N}$ and $m \neq n$

Ans:– WLOG $m > n$ $\quad \gcd(2^{2^n}+1, 2^{2^m}+1)$

Suppose p is any prime that divides $2^{2^n}+1$

$p \mid (2^{2^n}+1) \Rightarrow \quad 2^{2^n} = kp - 1$

$2^{2^{n+1}} = 2^{2^n \cdot 2} = (2^{2^n})^2$

$(a^b)^c = a^{bc}$

$= (kp-1)^2 = k^2p^2 - 2kp + 1$

$= p k' + 1$

$2^{2^{n+1}} = pk' + 1$

$m > n$

$\gcd(2^m+1, 2^n+1) \neq 1$

$= \gcd(2^m - 2^n, 2^n+1)$

$= \gcd(2^n(2^{m-n}-1), 2^n+1)$

$= \gcd(2^{m-n}-1, 2^n+1)$

$= \gcd(2^{m-n}-1, 2^n+1+2^{m-n+1}-2)$

$m=3,\ n=1$

$\gcd(9, 3) = 3 \neq 1$

$\gcd(2^m-1, 2^n-1) \quad m, n \in \mathbb{N}$

$= a^{b-}$

$$2^{2^{n+1}} = pk' + 1$$

$$2^{2^{n+2}} = (pk'+1)^2 = pk'' + 1$$

$m > n$ let $m = n + c$, $c \in \mathbb{N}$

$$2^{2^m} = 2^{2^{n+c}} = pk_c + 1$$

$\Rightarrow p \mid (2^{2^m} - 1)$

Suppose $p \mid (2^{2^m} + 1)$ $\Rightarrow p \mid (2^{2^m} + 1 - (2^{2^m} - 1))$

$\Rightarrow p \mid (2) \Rightarrow p = 2$

But $2^{2^m} + 1$ is odd so p cannot be 2 $\Rightarrow\Leftarrow$ Contradiction

So $p \nmid (2^{2^m} + 1)$ for any prime $p \mid (2^{2^n} + 1)$

$\Rightarrow 2^{2^m} + 1$, $2^{2^n} + 1$ are coprime

$\gcd(2^m - 1, 2^n - 1)$ $m, n \in \mathbb{N}$

$= 2^{\gcd(m,n)} - 1$

$= 1$ if m, n are coprime

$p \mid a$ & $p \mid b$

$\Rightarrow p \mid (a - b)$

Bézout's Theorem:-

Let a, b be integers. Then the equation $ax + by = n$ has a solution if and only if $\gcd(a,b) \mid n$. $(x, y \in \mathbb{Z})$

General Bézout's Identity:-

For integers $a_1, a_2, \dots, a_n$ there exists $x_1, x_2, \dots, x_n$ such that

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = \sum_{i=1}^{n} a_ix_i = \gcd(a_1, a_2, \dots, a_n)$$

Proof:- $a_1x_1 + a_2x_2 = \gcd(a_1, a_2)$ ... [using Bezout's identity]

Idea:- Then, $(a_1x_1 + a_2x_2)k_1 + a_3x_3 = \gcd(a_1, a_2, a_3)$

$a_1x_1' + a_2x_2' + a_3x_3 = \gcd(a_1, a_2, a_3)$ and so on

Q> For how many values of k is 12^{12} the LCM of 6^6, 8^8 and K, $k \in \mathbb{Z}$

Ans:- Home Work

Q> Find all positive integers n such that

$$(3^{n-1} + 5^{n-1}) \mid (3^n + 5^n)$$

Ans:- Home Work

Q> Home Work:- Read about Fibonacci Sequence in Wikipedia

Prove that two consecutive terms in Fibonacci sequence are coprime